UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/813,910	03/21/2001	Edward B. Boden	END9 2000 0093 US1	4675

7590 08/05/2005

IBM CORPORATION-DEPT. 917
3605 HIGHWAY 52 NORTH
ROCHESTER, MN 55901-7829

EXAMINER	
RYMAN, DANIEL J	

ART UNIT	PAPER NUMBER
2665	

DATE MAILED: 08/05/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/813,910	BODEN ET AL.	
	Examiner	Art Unit	
	Daniel J. Ryman	2665	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *30 June 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,3-14 and 16-22* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,3-14 and 16-22* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Response to Arguments

1. Applicant's arguments with respect to claims 1 and 3-14, and 16-22 have been considered but are moot in view of the new ground(s) of rejection.

Specification

2. The disclosure is objected to because of the following informalities: on page 12, line 6 "processing and" should be "processing an"; and on page 13, line 18 "or" should be "for".

3. Appropriate correction is required.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 1, 3-14, and 16-22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Srisuresh (P. Srisuresh. "RFC 2709 – Security Model with Tunnel-mode IPsec for NAT Domains". Network Working Group, RFC 2709. October 1999. pages 1-9 in view of Applicant's Admitted Prior Art.

6. Regarding claims 1 and 10, Sresuresh discloses a method and system for operating a first node in a network including at least one second node, the method comprising the steps of and the system comprising means for: establishing at said first node a coincident endpoint (tunnel end point) for an outer connection (IPsec connection, output encapsulation of tunnel packet) and an inner connection (private connection, inner encapsulation of tunnel packet) with respect to at

least one second node (pages 1-2, sections 1 and 2.2); responsive to receiving an inbound nested (embedded or tunneled) packet (IPsec packet) from said second node on said outer connection, decapsulating said packet into a first packet (private packet) and then performing source-in network address translation on said first packet (page 4, Figure 4) where NAT translates the source addresses of the private network device (source address of private network is not globally unique such that it must be translated) (page 3, section 3) such that, as broadly defined, the NAT is source-in NAT; and responsive to receiving an outbound second packet (private packet) at said inner connection, performing source-in network address translation on said second packet, and then encapsulating said second packet into a nested packet (IPsec packet) for communication on said outer connection to said second node (page 4, Figure 3) where NAT translates the source addresses of the private network device (source address of private network is not globally unique such that it must be translated) (page 3, section 3) such that, as broadly defined, the NAT is source-in NAT.

Sresuresh does not expressly disclose that the outer connection and the inner connection are both IP security connections; however, Sresuresh does disclose that the outer connection is an IP security connection (page 3, section 3). Applicant admits as prior art that it is well known to have both an outer connection and an inner connection be IP security connections in order to permit a remote user to connect to an enterprise using a VPN (page 2, line 7-page 4, line 14). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to have the outer connection and the inner connection be IP security connections in order to permit a remote user to connect to an enterprise using a VPN.

7. Regarding claim 3, Sresuresh discloses, in a particular embodiment where an IKE process is used, a method for managing connections within a communications system, comprising the steps of: configuring an outer connection (connection over public network between peering node and gateway) (pages 1-2, section 1 and pages 2-3, section 2.2); communicating from a client (peering node) to a gateway on said outer connection a request to configure an inner connection (IKE communications) (pages 5-6, section 4 and Fig. 5); responsive to said request, initializing said gateway to receive a future nested communication, including obtaining a client address from a packet on said outer connection (pages 5-6, section 4 and Fig. 5); starting said inner connection (tunneled connection between private network and public node) (pages 3-4, section 3); responsive to starting said inner connection, propagating a network address translation rule from said outer connection to said inner connection (pages 3-5, sections 3 and 4 and Figs. 3 and 4) where the inner connection and outer connection will need to know the NAT translations in order to ensure that an inbound packet is correctly translated between the outer connection and the inner connection and an outbound packet is correctly translated between the inner connection and the outer connection.

Sresuresh does not expressly disclose that the outer connection and the inner connection are both IP security connections; however, Sresuresh does disclose that the outer connection is an IP security connection (page 3, section 3). Applicant admits as prior art that it is well known to have both an outer connection and an inner connection be IP security connections in order to permit a remote user to connect to an enterprise using a VPN (page 2, line 7-page 4, line 14). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the

invention to have the outer connection and the inner connection be IP security connections in order to permit a remote user to connect to an enterprise using a VPN.

8. Regarding claim 4, Sresuresh in view of Applicant's admitted prior art discloses further responsive to starting said inner connection, encapsulating a packet outbound from said gateway first in said inner connection and then in said outer connection (Sresuresh: pages 3-4, section 3).

9. Regarding claim 5, Sresuresh in view of Applicant's admitted prior art discloses responsive to receiving a packet at said gateway, determining if said packet has a security header (Sresuresh: pages 3-4, section 3 and Fig. 4); responsive to said packet having said security header, decapsulating said packet (Sresuresh: pages 3-4, section 3 and Fig. 4) and saving any address translation rule included within said packet (Sresuresh: pages 4-5, section 4, lines 24-59); and applying said address translation rule to said packet and thereafter communicating said packet from said gateway to said client (Sresuresh: pages 3-4, section 3 and Fig. 4).

10. Regarding claim 6, Sresuresh in view of Applicant's admitted prior art discloses iteratively executing said decapsulating step until a resulting decapsulated packet no longer contains a security header (Sresuresh: pages 3-4, section 3 and Fig. 4) where, as broadly defined, the decapsulation is performed until there are no more security headers.

11. Regarding claim 7, Sresuresh discloses a method for enabling a local gateway to handle IP addresses from remote clients, comprising the steps of: assigning said IP address to a remote client (pages 3-5, sections 3 and 4); automatically maintaining between said remote client and said gateway nested connections with local coincident endpoints (pages 3-5, sections 3 and 4). Sresuresh also discloses as a possible application that the IP addresses can be dynamically assigned IP addresses (temporary service provider assigned address) (pages 6 and 7, section 5.2).

Thus, it would have been obvious to one of ordinary skill in the art at the time of the invention to have the IP addresses be dynamically assigned IP addresses since this is part of a possible application.

Sresuresh does not expressly disclose that the outer connection and the inner connection are both IP security connections; however, Sresuresh does disclose that the outer connection is an IP security connection (page 3, section 3). Applicant admits as prior art that it is well known to have both an outer connection and an inner connection be IP security connections in order to permit a remote user to connect to an enterprise using a VPN (page 2, line 7-page 4, line 14). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to have the outer connection and the inner connection be IP security connections in order to permit a remote user to connect to an enterprise using a VPN.

12. Regarding claim 8, Sresuresh in view of Applicant's admitted prior art discloses that said nested connections comprise an inner connection and an outer connection (Sresuresh: pages 3-5, sections 3 and 4 and Applicant: page 2, line 7-page 4, line 14).

13. Regarding claim 9, Sresuresh in view of Applicant's admitted prior art discloses responsive to receiving an inbound nested packet from said client on said outer connection, decapsulating said packet into a first packet and then performing source-in network address translation on said first packet (Sresuresh: pages 3-4, section 3 and Fig. 4) where NAT translates the source addresses of the private network device (source address of private network is not globally unique such that it must be translated) (Sresuresh: page 3, section 3) such that, as broadly defined, the NAT is source-in NAT; and responsive to receiving an outbound second packet at said inner connection, performing source-in network address translation on said second

packet, and then encapsulating said second packet into a nested packet for communication on said outer connection to client (Sresuresh: pages 3-4, section 3 and Fig. 3) where NAT translates the source addresses of the private network device (source address of private network is not globally unique such that it must be translated) (Sresuresh: page 3, section 3) such that, as broadly defined, the NAT is source-in NAT.

14. Regarding claims 11 and 16, Sresuresh discloses performing NAT in tunneled connections (page 3-5, sections 3 and 4). Sresuresh also discloses that one application of the NAT in tunneled connections is in VPNs (pages 6-7, section 5.2), such that it would have been obvious to one of ordinary skill in the art at the time of the invention to apply the NAT in tunneled connections to a VPN. Thus, Sresuresh discloses a method and system for extending virtual private network (VPN) network address translation (NAT) to include support for nested connections with coincident endpoints (tunnel end points), without requiring any special configuration for the inner (nested) VPN connection, with respect to VPN NAT (pages 3-7, sections 2.2, 3, 4, and 5.2), the method comprising the steps of and the system comprising means for: configuring an outer connection with a VPN NAT rule (connection over public network between peering node and gateway) (pages 1-2, section 1 and pages 2-3, section 2.2); communicating from a client (peering node) to a gateway on said outer connection a dynamically generated security association request packet to configure a secure inner connection (IKE communications) (pages 5-6, section 4 and Fig. 5); responsive to said request, initializing said gateway to receive a future nested communication, including obtaining a client address from said request packet on said outer connection (pages 5-6, section 4 and Fig. 5); starting said inner connection (tunneled connection between private network and public node) (pages 3-4, section

3); responsive to starting said inner connection, propagating said VPN NAT rule from said outer connection to said inner connection (pages 3-5, sections 3 and 4 and Figs. 3 and 4) where the inner connection and outer connection will need to know the NAT translations in order to ensure that an inbound packet is correctly translated between the outer connection and the inner connection and an outbound packet is correctly translated between the inner connection and the outer connection.

Sresuresh does not expressly disclose that the outer connection and the inner connection are both IP security connections; however, Sresuresh does disclose that the outer connection is an IP security connection (page 3, section 3). Applicant admits as prior art that it is well known to have both an outer connection and an inner connection be IP security connections in order to permit a remote user to connect to an enterprise using a VPN (page 2, line 7-page 4, line 14). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to have the outer connection and the inner connection be IP security connections in order to permit a remote user to connect to an enterprise using a VPN.

15. Regarding claim 12, Sresuresh in view of Applicant's admitted prior art discloses further responsive to starting said inner connection, encapsulating a packet outbound from said gateway first in said inner connection and then in said outer connection (Sresuresh: pages 3-4, section 3).

16. Regarding claim 13, Sresuresh discloses responsive to receiving a packet at said gateway, determining if said packet has a security header (pages 3-4, section 3 and Fig. 4); responsive to said packet having said security header, decapsulating said packet (pages 3-4, section 3 and Fig. 4) and saving any VPN NAT rule included within said packet (pages 4-5, section 4, lines 24-59);

and applying said NAT rule to said packet and thereafter communicating said packet from said gateway to said client (pages 3-4, section 3 and Fig. 4).

17. Regarding claim 14, Sresuresh in view of Applicant's admitted prior art discloses iteratively executing said decapsulating step until a resulting decapsulated packet no longer contains a security header (Sresuresh: pages 3-4, section 3 and Fig. 4) where, as broadly defined, the decapsulation is performed until there are no more security headers.

18. Regarding claims 17 and 18, incorporating the rejection of claims 1 and 10, Sresuresh in view of Applicant's admitted prior art discloses all of the limitations of claims 17 and 18, as outlined in the rejection of claims 1 and 10, except having a program storage device readable by a machine, tangibly embodying a program of instructions executable by a machine to perform the method where the program operates a first node. Examiner takes official notice that it is well known in the art to use software to implement a method since software is very flexible. Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to have a program storage device readable by a machine, tangibly embodying a program of instructions executable by a machine to perform the method where the program operates a first node since software is very flexible.

19. Regarding claims 19-22, incorporating the rejection of claims 3-6, Sresuresh in view of Applicant's admitted prior art discloses all of the limitations of claims 19-22, as outlined in the rejection of claims 3-6, except having a program storage device readable by a machine, tangibly embodying a program of instructions executable by a machine to perform the method. Examiner takes official notice that it is well known in the art to use software to implement a method since software is very flexible. Therefore, it would have been obvious to one of ordinary skill in the art

at the time of the invention to have a program storage device readable by a machine, tangibly embodying a program of instructions executable by a machine to perform the method since software is very flexible.

Conclusion

20. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Daniel J. Ryman whose telephone number is (571)272-3152. The examiner can normally be reached on Mon.-Fri. 7:00-4:30 with every other Friday off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Huy Vu can be reached on (571)272-3155. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Daniel J. Ryman
Examiner
Art Unit 2665

HUY D. VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2600